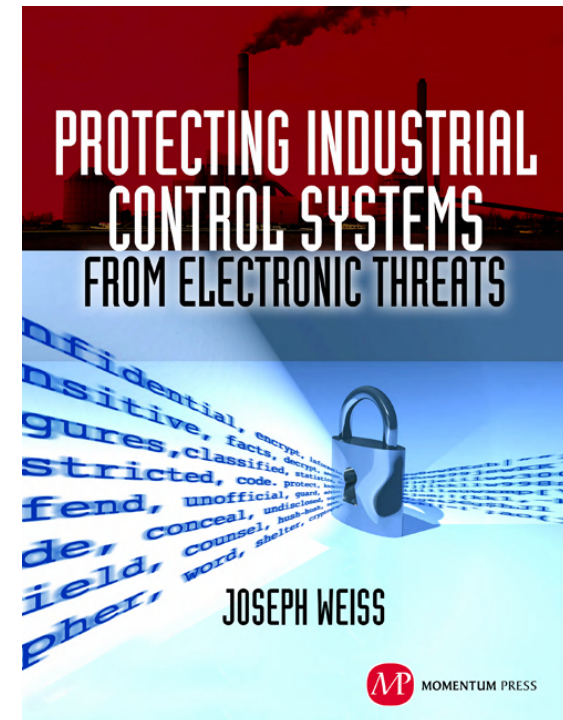


r Security of Industrial Control Systems

A Status Report

October 12, 2011

Joe Weiss, PE, CISM
(408) 253-7934
joe.weiss@realtimeacs.com



ISBN: 978-1-60650-197-9

Definitions that can be Confusing

- SCADA
- ICS
- Security
- Fail-Safe
- Denial-of-Service
- IDS
- IED
- Redundancy
- Reliability/Safety/Security
- Unnecessary ports and services

Background

- Industrial control systems (ICSs) operate power, water, chemicals, pipelines, etc
- ICSs include SCADA/EMS, DCS, PLCs, RTUs, IEDs, smart sensors and drives, emissions controls, equipment diagnostics, AMI (Smart Grid), programmable thermostats, building controls,...



FIPS Cyber Incident Definition

- Cyber Incident - An occurrence that actually or potentially jeopardizes the Confidentiality, Integrity, or Availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional. (FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System*, March 2006.)
 - What is important about this definition
 - Intentional or unintentional
 - Actual or potential compromise of CIA
 - Violation or imminent threat to CIA

What has happened since last year

- Brazilian control system network infections
- Russian Sayano–Shushenskaya Dam failure
- ExxonMobil Yellowstone River gasoline pipeline break
- China bullet train crash
- BART shutdown
- Chile electric outage
- San Diego outage (?)
- BP Deepwater Horizon report
- Other non-public ICS cyber incidents
- Issues with separation of control and safety systems
- Disclosure issues
- Equipment certification starting
- Confusion with San Bruno
- Legislation
- Nation-state threats to attack ICSs
- ICS metasploits now available

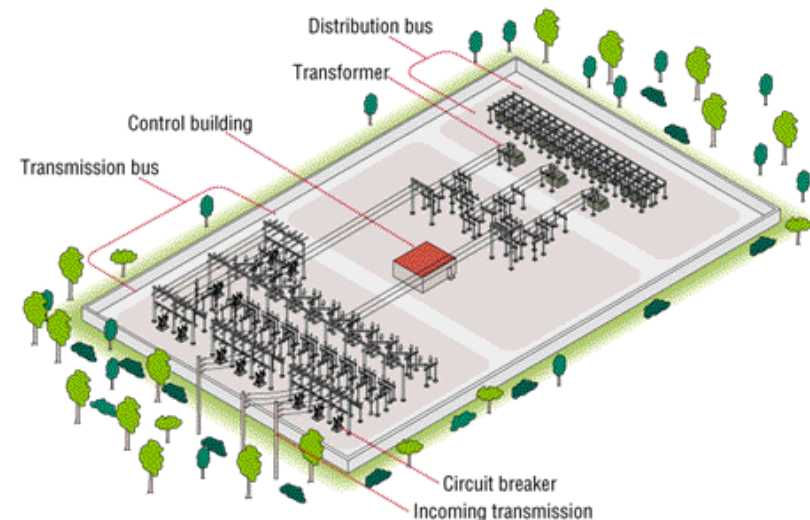
Sample Linked-In Threads of Interest

- **Does iPad have a place in an Automation Engineers toolbox? (Automation & Control Engineering)**
 - I have been looking at different business uses for the iPad and would like to start a discussion around using the iPad as a tool to help the Automation Engineer in their day to day work.
- **What kind of technology or functionality do you need or expect in new DCS systems in 5 to 10 years? (DCS Selection and Reliability)**
 - For example Faster I/O scan rates, COTS I/O modules, high density I/O, New kind of field busses, wireless systems et cetera, 3d Screens, more integration between desk and field operators and maintenance teams.
- **Does anybody know a real Control system project which runs under Linux? (Automation and Control Engineering)**
 - Ovation has a version that runs on (Sun) Solaris. But on the other hand, Emerson released last version on February and will not be issuing more releases. Since the current trend in the automation market is Windows-based systems, nearly all DCS companies are no longer offering UNIX based solutions.



Brief History of ICS

- 20 years ago – Isolated systems, with non-networked cyber “dumb” devices
- 10 years ago – Emergence of network integration, with more capable “intelligent” cyber-vulnerable devices
- Today – Combination of modern, integrated networks interoperating with legacy systems creating increasingly cyber-vulnerable networks
- 10 years from now – Who knows? Expect further convergence of networked legacy, intelligent, and newer technologies, with even more cyber vulnerability



Control Systems Basics

Sensors



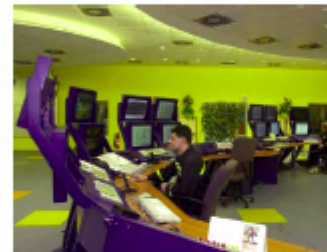
Control Valves



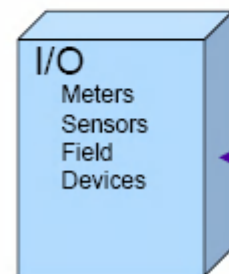
Programmable Logic Controllers (PLC)



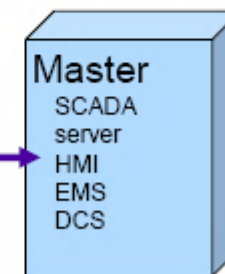
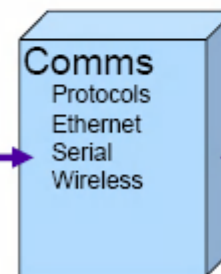
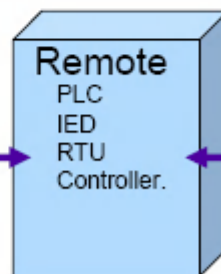
Human Machine Interfaces (HMI) and Operator Displays



Motor Controls



Field Devices



Control Center

Slide courtesy of Anixter © Proprietary 04-2009

Evolution 1- *Panel based Controls*

- Push Buttons
- Single Loop Controls
- Stand Alone
- No Networks
- No Communication

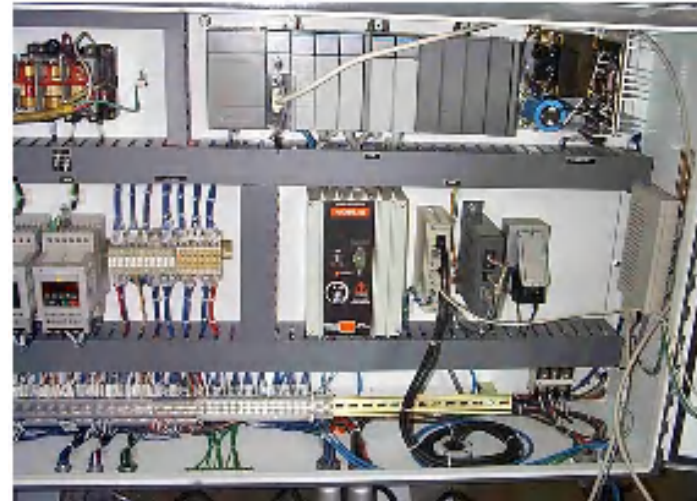
From a cyber security standpoint this system is *isolated and “cyber-dumb”*



Slide courtesy of Anixter © Proprietary 04-2009

Evolution 2 - Legacy Electronic Controls

- Proprietary Networks
- Proprietary OS
- No Ethernet
- No Internet connections
- No Intranet connections
- “Security by Obscurity”



From a cyber security standpoint this system is cyber vulnerable

Slide courtesy of Anixter © Proprietary 04-2009

Evolution 3- Modern Technology

- Ethernet everywhere
- Wireless 'in the rack'
- Remote configuration
- Windows & Linux OS
- Commercial Off The Shelf (COTS)

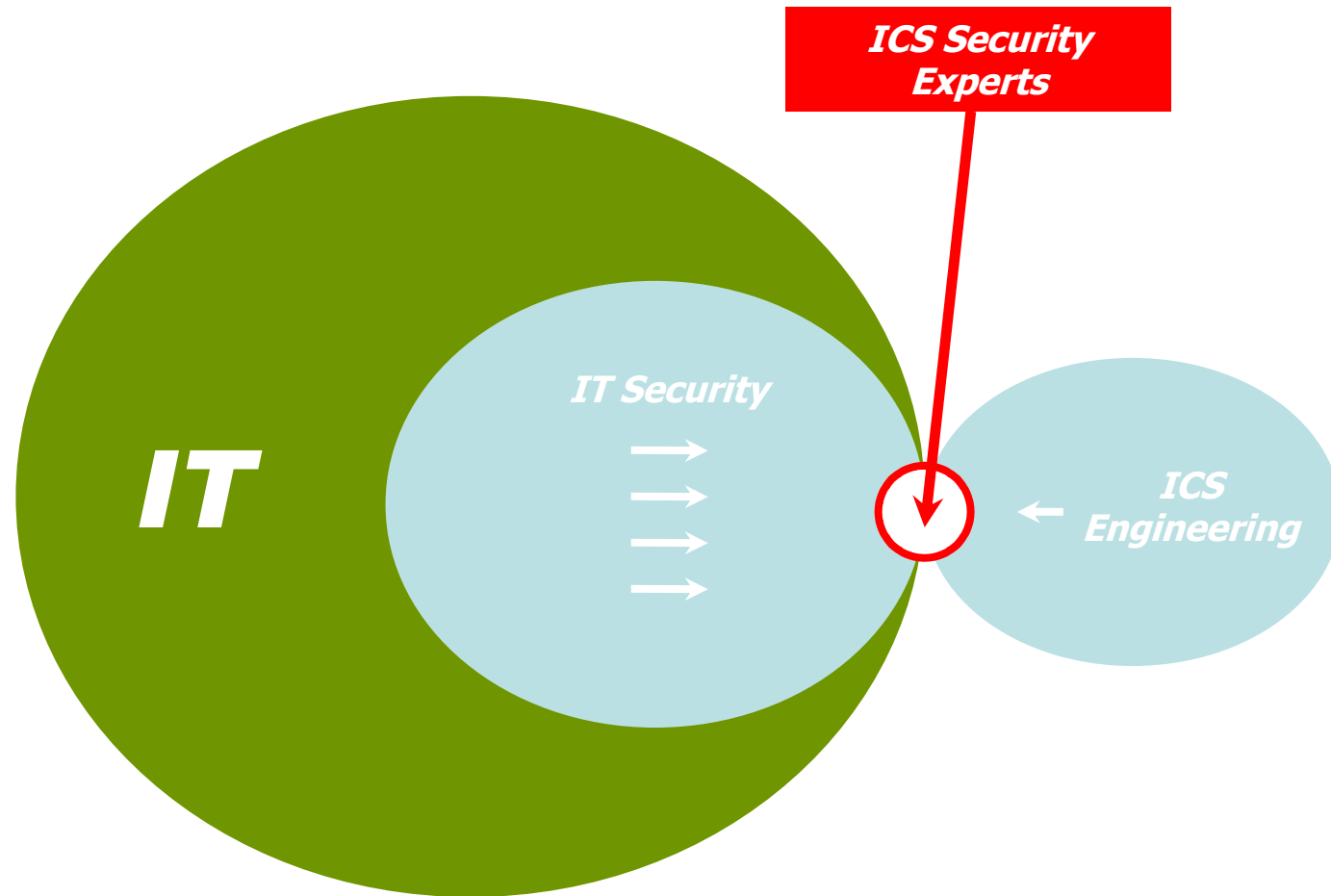


From a cyber security standpoint this system is very cyber vulnerable



Slide courtesy of Anixter © Proprietary 04-2009

ICS Security Expertise Lacking



Myths

- The Internet and Microsoft are biggest ICS cyber threats
- Using Windows and TCP/IP “make it IT”
- External malicious threats are the biggest concerns
- Firewalls, VPN/encryption make you secure
- ICS Code insertion can be found by AntiVirus
- IDS will identify ICS attacks
- Field devices can’t be hacked
- Can’t use dial-ups or default passwords
- You are secure if hackers can’t get in
- More and better “widgets” can solve all our security problems
- “If we keep our head down they won’t find us”



Lonnie Carter
President & CEO
Santee Cooper
Moncks Corner, S.C.



Robert Johnston
President & CEO
MEAG Power
Atlanta



Gary Stauffer
Executive Director
NMPP Energy
Lincoln, Neb.



Lynne Tejeda
General Manager & CEO
Keys Energy Services
Key West, Fla.

lines rated to withstand winds of 150 miles per hour. That means using very large concrete poles.

ENERGYBIZ: What is your response to concerns about grid cyber security?

JOHNSTON: There's been an awful lot written about cyber security and the threat of it. There are a lot of people who want to spend a huge amount of money on something that we have not necessarily identified. There have been some hackings into some certain systems around the country, but show me an event where we've lost systems due to cyber terrorism. I'm not aware of one.

CARTER: There's not a utility in this country that does not do everything possible to keep its system reliable, and that would not act on any threat that it understood and had a way to mitigate or eliminate it. Explain the threat to us and we will go work on it. Congress is going to have to decide who in our government is responsible for identifying and communicating those threats to us.

ENERGYBIZ: In addition to focusing on cyber security, the government is forging new guidelines for dealing with risk.

STAUFFER: We have effectively traded and hedged and have done very sophisticated swaps on the gas side for many years, and have been very successful. We also are very careful that we never have any open-ended commitments. Unfortunately, I think we're going to get swept up in the frenzy about unmitigated risk taken by people who are financial players and not commodity users. Potentially, the credit requirements that will be imposed on us will limit our ability to manage our business. I'm worried that what happened on Wall Street in a liquidity crisis is going to end up in a credit crisis for small towns, municipalities and villages in the heartland.

ENERGYBIZ: How are power markets functioning today?

CARTER: Capacity is not being built. The incumbents are not encouraged by the market to build because if supply is less than the demand, the price goes up. We see places like New Jersey trying to take action to ensure that capacity is actively installed and added to these markets. These markets have failed to produce the promised benefit to consumers. The APPA has made some suggestions to the Federal Energy Regulatory Commission and others to reform markets, and those suggestions have gone unaddressed. Now what we see is that several states are taking some of the matters into their own hands to ensure that additional capacity gets put into those markets.

STAUFFER: What worries me is what's just occurred in the forward capacity auction in the PJM Interconnection. It looks like we would not be able to have any right to self-generation in the capacity market. Clearly, it needs work.

ENERGYBIZ: What disruptions in your business do you fear?

TEJEDA: Hurricanes. You can't plan for them, and they take away all your ability to plan.

JOHNSTON: We serve 49 cities throughout the state of Georgia and the most disruptive thing for us is the economic downturn that's been very uneven across those 49 communities.

CARTER: Regulation without a doubt is the thing that is the most disruptive for our business.

STAUFFER: The most disruptive situation we're facing is externally imposed political mandates relative to decision-making on what portfolio we will put together to supply power. ☐

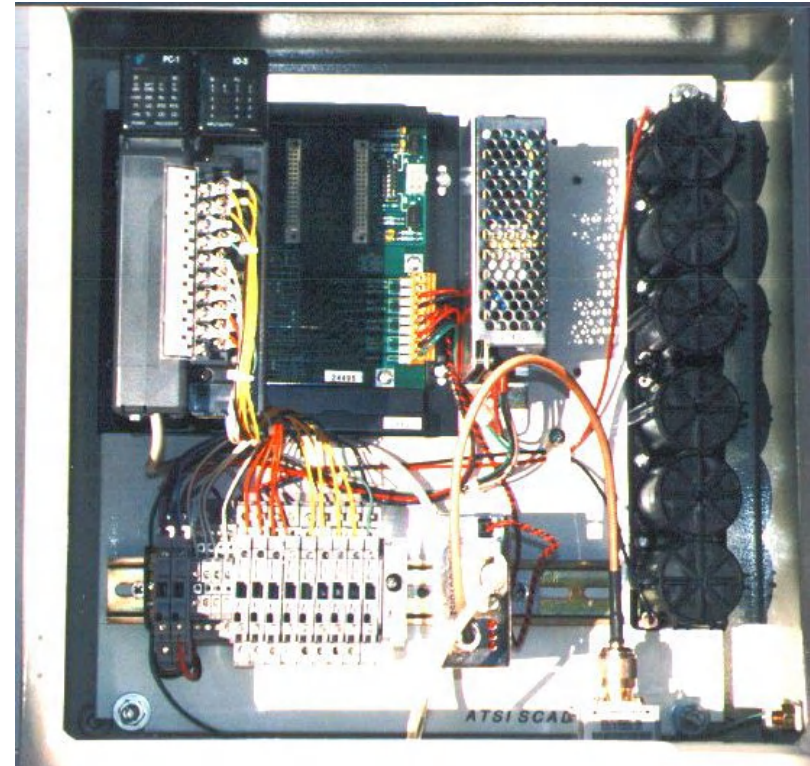
energybiz.com ENERGYBIZ 35

Is AntiVirus Sufficient for ICS?

- Anti-Virus is pattern recognition and can only recognize known patterns
- Examples where Antivirus hasn't worked to protect ICS networks:
 - Stuxnet
 - Others (presentation and video by Marcelo Branquinho)
 - These attacks are against fully patched systems with current AV signatures. They succeed because of the encoding capability in attack tools like metasploit makes the payloads look unique to the AV system.

ICS Cyber Issues

- ICS designs did/do not include security – it's a back-fit
 - Many new systems cyber vulnerable
- System integration with insecure systems
- Lack of ICS cyber forensics
- Culture
 - Operations considers security a pain



ICS Vendor Cyber Issues

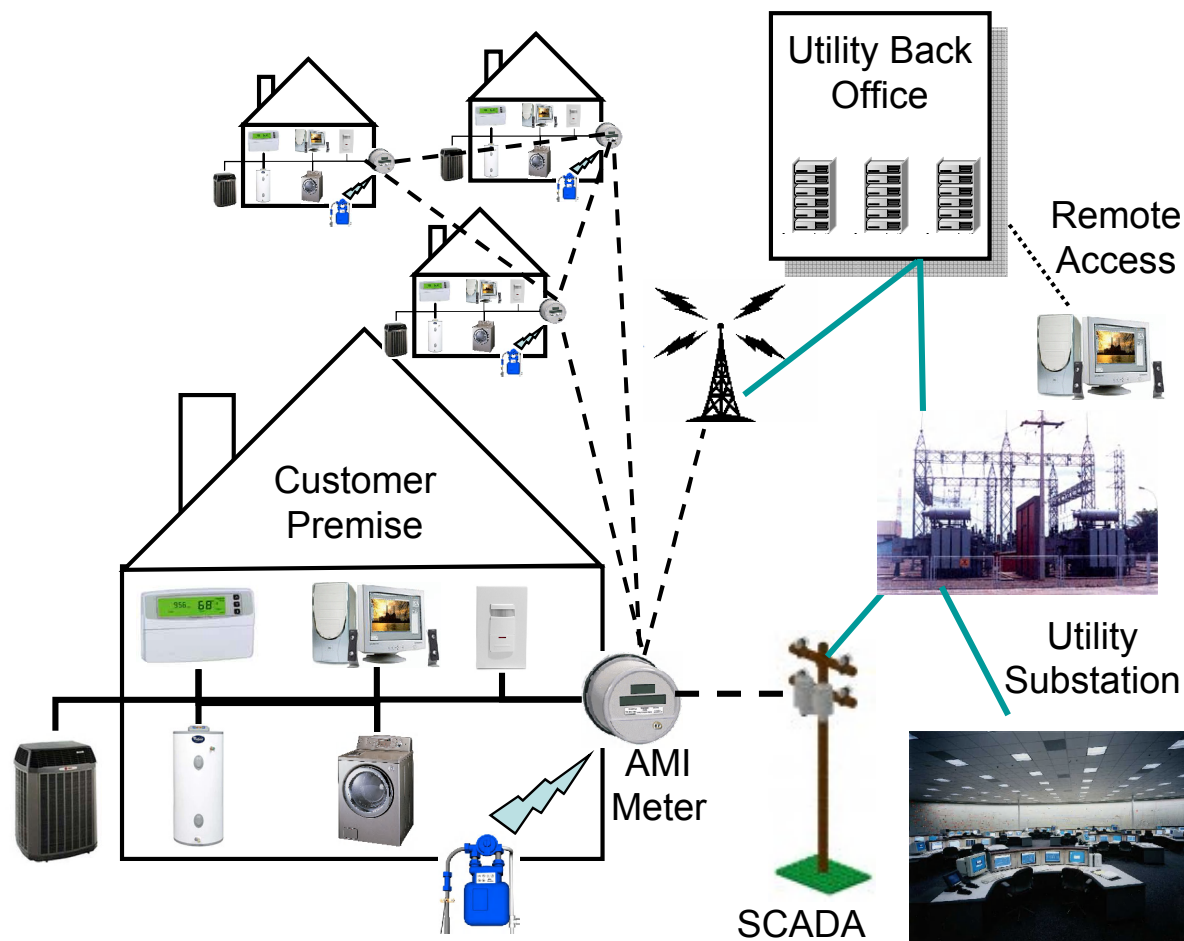
- Modern wind farms have interactive control capabilities
 - Built-in WiFi, GPRS with sim-cards, RS232 comports for external RTU
 - Local Mini-SCADA with direct access to regional control
- Some smart grid vendors using bluetooth and “embedded” modems
- Other ICS vendors using wireless modems



* Wind Power Communications Security Concerns and Protection

Gary Seifert, Idaho National Laboratory

Big Push for Smart Grid



Unique Smart Grid Cyber Threats

- Privacy
- Vastly expanded threat space
- Blurring of IT and ICS
- Public awareness of vulnerabilities

ICS Cyber Incidents

- 200+ incidents world-wide
 - Most unintentional
 - Some malicious attacks
 - Impacts range from trivial to major outages to deaths
 - Most not identified as cyber
 - DOD caused some
- ICS incidents may not violate IT security policies



Targeted SCADA Attack

- Insecure system integration enabled targeted attack
- No SCADA servers or mapping system for two weeks
- 4 Man-months to recover
- Minimal forensics
- No information sharing with local law enforcement, FBI, or ES-ISAC



Stuxnet – Root Kit

Pipeline Ruptures



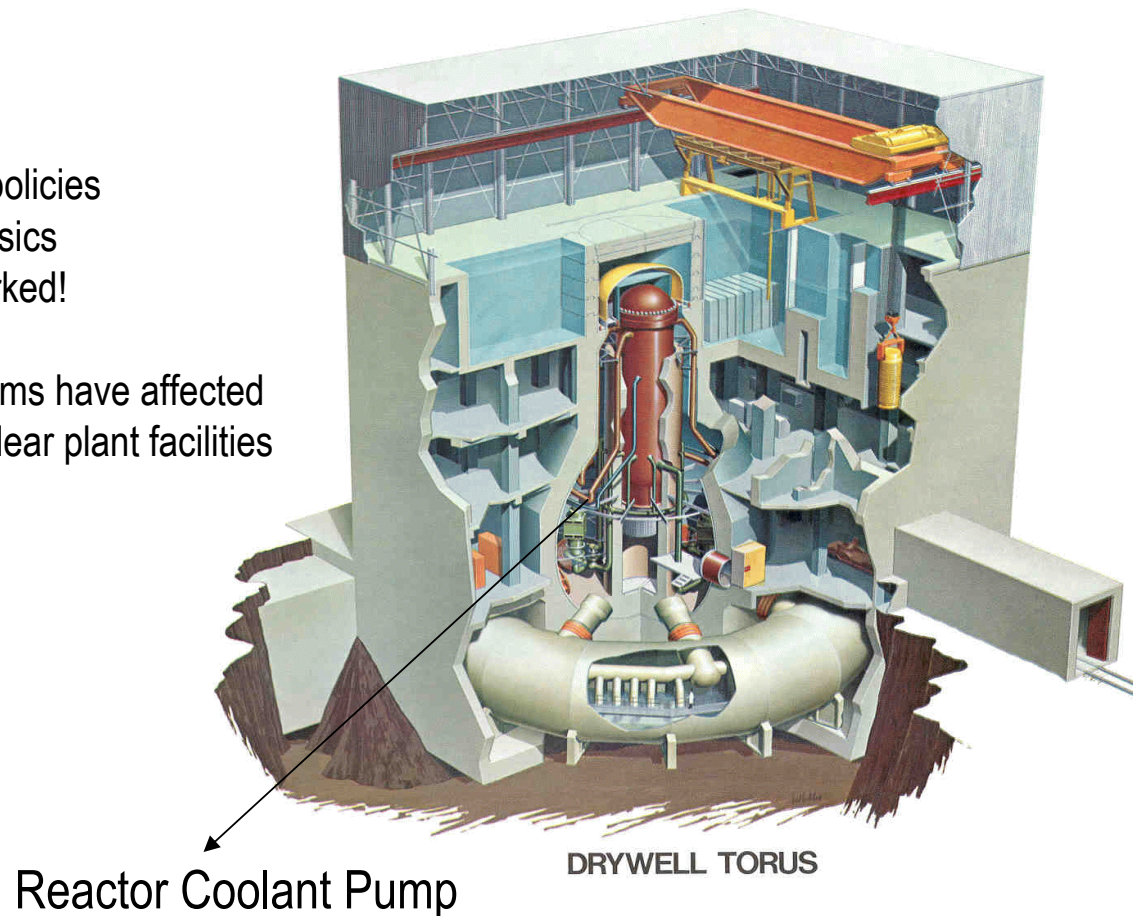
June 1999 Bellingham, WA



September 2010 San Bruno, CA

Nuclear Plant Cyber Incidents

- Inadequate policies
- Lack of forensics
- Failsafes worked!
- Same problems have affected many non-nuclear plant facilities



GENERAL ELECTRIC

GEZ-4396

DC Metro Crash

- June 22, 2009 DC Metro trains collided
- 9 dead, 52 injured
- System consisted of sensors, RTUs, and SCADA
 - Previous unresolved problems
 - Lack of sensor data and alarms
- November 29, 2009 DC Metro train crash



Unintended Consequences

- A disturbance **caused by the implementation of a device locking security tool** resulted in the loss of SCADA services. The tool was being implemented in response to the NERC CIP standards.

From January-June 2009 NERC
Disturbance Reports



Other Concerns

- Lack of personnel certifications
 - Neither PE nor CISSP adequate
- Lack of university interdisciplinary courses
 - Need in both computer science and engineering
- Lack of understanding/denial
 - Based on presentations, articles, and NERC CIP process

Recommendations

- Get senior management buy-in
- Get the right people involved
- Understand what you have installed
- Develop appropriate policies and procedures
- Implement appropriate technologies that won't affect system performance or compromise safety
- Make it a living program
- Work with IT to know when a sophisticated attack has occurred

Conclusions

- Can not fully secure ICSs
 - Worry about intentional and unintentional
 - Need graceful degradation
 - Need to be able to recover
- Threats are real
 - Lack of forensics complicates recovery and prosecution
- Need appropriate knowledge